EXHIBIT 8

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

| | | |
|---|---|---|
| CHRISTOPHER HOWE, individually and on behalf of all others similarly situated, | ) | |
| Plaintiffs, | ) | |
| vs. | ) | Case No. 1:19-cv-01374 |
| SPEEDWAY, LLC, | ) | |
| Defendant. | ) | |

CONTAINS PORTIONS PRELIMINARILY
DESIGNATED CONFIDENTIAL

The expert deposition of CHRISTOPHER DAFT, Ph.D., taken remotely via Zoom, called by the Defendant for examination, taken pursuant to the Federal Rules of Civil Procedure of the United States District Courts pertaining to the taking of depositions, taken before Marianne Nee, a Certified Stenographic Reporter of the State of Illinois, CSR License No. 084-002341, taken on Friday, September 24, 2021, commencing at 10:02 a.m. Central Time.

CASE NO. 40835

PROCEEDINGS:

* * *

(Witness sworn/affirmed.)

CHRISTOPHER DAFT, Ph.D.,

called as a witness herein, having been first duly sworn/affirmed, was examined and testified as follows:

EXAMINATION

BY MR. WOLFE:

Q. Good morning, Dr. Daft.

A. Good morning.

Q. Could you state your name for the record, please?

A. Yes. My full name is Christopher Mark William Daft.

Q. Have you ever had your deposition taken before?

A. Yes, I have.

Q. How many times?

A. I believe it's six times.

Q. You understand that you are under oath today and your testimony needs to be truthful just as it would if you were in front of a judge or jury?

A. Depending on how fast you can place your finger. I mean, it depends on how many fingers you want to enroll and how rapidly you can change your position, the position of your fingers for it to do -- I mean, it has to do multiple acquisitions with different orientations of the fingers. So that's why I'm saying it could vary.

Q. I understand. I asked you a bad question. I want to ask a little bit different question. Fingerprint enrollment, it says image acquisition, image processing, feature extraction, template generation.

From the time that a person puts their finger on the sensor and the image is acquired until the time that a template is generated -- I'm talking about just one touch -- how long does that process take?

A. That's very fast. Less than a second.

Q. Less than a half of a second?

A. I think so.

Q. Less than a quarter second?

A. That depends on the speed of the phone's processor, but the user experience requires that it be fast.

Q. Is that true of other fingerscan technology commonly used in consumer products as well?

A. The Touch ID is also fast at that process.

Q. Based on your experience working on the Qualcomm phone, it would have been unacceptable if the enrollment of a single fingerscan took more than a half a second, right?

A. Yes. In a consumer electronics device, you don't want the user experience to be tiresome. So I certainly would say that if each image acquisition were taking five seconds, this would not be a user experience that would be competitive.

Q. And what is actually stored in the database is a template, right?

A. That's correct.

Q. The image is not stored in the database?

A. That's correct.

Q. Would there be practical reasons that you wouldn't want to store the image in the database?

A. Yes.

Q. What are they?

A. A template is simply a set of features extracted from the fingerprint, and that can be considerably smaller than the fingerprint image, so it makes engineering sense to store the smaller representation.

Q. Do you know how many bytes a template is typically made up of?

A. Well, it depends on how rich you want the representation of the fingerprint to be.

Q. The template on the Qualcomm phone, do you know how many bytes it takes up?

A. I think it's a kilobyte, something in that range.

Q. One kilobyte?

A. Yes.

Q. In the scheme of templates, is that a big one or a small one?

A. I think it's normal. The point is that it captures enough -- I mean, it -- you can think of it as a digit compression, you know, like you do a zip file, you do a zip operation

Q. Does the Qualcomm product, does it hold an entire image or does it process it through segments?

A. It acquires the fingerprint image and then it does -- let me start again. It acquires the ultrasound data.

It processes that into a fingerprint image, and then the cleanup process we've been discussing is applied and then the template is made. So it's an image up to the feature extraction.

Q. Is it fair to say that -- never mind. I already asked that question. I'm not going to waste your time.

Just to make sure that we understand each other, what does the term feature extraction mean to you?

A. It means taking the fingerprint image and extracting data that has the essence of the image in it but is smaller.

Q. And what does the term template generation mean to you?

A. That is making the small binary file which gets stored in the database and uses it for matching.

Q. Is it your opinion that there is no difference between a template and a fingerprint image like the one that you captured in the Qualcomm device?

A. That's not my opinion, no.

Q. What is the difference?

A. The difference -- well, there are several differences. The template must capture the essence of the fingerprint in order for the device to function, but the template is considerably smaller than the fingerprint image.

Q. And when you say considerably smaller, what do you mean?

A. I mean that the fingerprint image might be hundreds of kilobytes when it comes out of the image processing block in the finger we're looking at, whereas the template is perhaps 100 times smaller.

Q. And what happens that makes the template 100 times smaller than the fingerprint image?

A. What happens that makes it a lot smaller is that the feature extraction is finding the key characteristics of the fingerprint image and retaining only those characteristics.

Q. Did you have any involvement in any biometric security aspect of the Qualcomm products?

A. The initial device was actually I believe aimed at government customers, so there was a small amount of discussion at the beginning of the project about whether, you know, this was going to be something developed for law enforcement, and the decision was then taken to only focus on the consumer device.

Q. I'm sorry. I must have asked a bad question. My question is, did you have any involvement in the biometric security aspect of the product, by which I mean encryption or other things meant to keep the data secure?

A. No. That's really on the -- that's the part which was done by the Qualcomm group that I didn't interact with.

Q. You said you worked on the Qualcomm project for about two years.

A. Yes, something like that. Maybe two or voltage for example. But I should qualify this because in recent years in engineering there has been an enormous amount of work on systems that produce all of the data that we want, so a complete fingerprint image without distortion, while they do not conform to the Nyquist requirement. So I don't -- so classically, historically, Nyquist requirement is a huge deal. In recent years people have been finding ways around this.

Q. What are the ways around it?

A. So there is a technique in engineering called compressed sensing. What compressed sensing means is acquiring data that doesn't conform to Nyquist and nevertheless getting all of the information out of -- let me put it in our context -- getting all of the fingerprint information that there is.

So compressed sensing is an engineering technique that is currently on file because it turns out that conforming to the Nyquist requirement has a large bearing on the cost of devices.

So basically what I'm saying is

classically Nyquist tells you how you sample in space and in time, but it's not fair to say that that is a completely rigorous requirement that if you don't meet it, your device stops working. That is not -- that is not true.

Q. What is the status of these new methods that people are developing to get around the Nyquist theorem?

A. They are involved -- they are using a variety of products already. For example, digital photography is using compressed sensing. So you get a photograph out of your digital camera that was not sent -- that was not sent at the Nyquist rate. The resolution of that photograph beats Nyquist.

Another example is diagnostic imaging. People are producing CT scans and particularly MRI scans when the dataset that's collected doesn't meet the Nyquist requirements, and still this is providing an image that a physician can use that doesn't have artifacts in it.

Q. What is the quality of the image that these methods provide?

A. They approach the data quality that you would get if you conformed to the Nyquist requirements.

Q. Do they provide the same data quality that you would get if you conformed to the Nyquist requirements?

A. That depends. You see, the acquired data always has some problems. For example, every sensor has noise in it. So it's not a perfect fingerprint no matter what you're -- no matter how good your electronics is. So every acquired image has imperfections.

What this compressed sensing part of engineering is finding is that they can get the artifacts produced by the compressed sensing by not obeying Nyquist below the other imperfections in the dataset. So at that point it's as good as a data acquisition that conforms to Nyquist.

MR. WOLFE: This would be a good time to take a lunch break. So do you want to take 45 minutes?

MR. FICZKE: 45, half an hour, whatever works for all you guys.

MR. WOLFE: Let's do 45.

compression for photographs.

I wouldn't call the operation of forming the template, it's not similar to JPEG compression. It's more a feature extraction. But the output is a representation of the key information that's in the image. So I guess the only thing I would say -- what I'd say no to in response to your question is it's not like doing JPEG compression.

Q. Do you understand that an algorithm is applied to the image as part of feature extraction and results in a template?

A. Yes. The template is a calculation based on the fingerprint image.

Q. Does the template contain all of the information originally in the fingerprint image?

A. It does not. It contains the essence of it.

Q. Does it contain actual images of those essences of a finger image or does it contain them, you know, by typology, you know, ridge ending of this sort in this location?

A. It's -- the template is the result of feature extraction and so the template is a list of features derived from the image.

Q. Can you explain to me the difference between identification and verification in the biometric context?

A. Yes.

Q. Please do.

A. The classic identification process is what the FBI does. The FBI has had for a long time the A-F-I-S system, and its purpose is to take fingerprint data and produce a name of a person. So that, as the name of the system implies, that's identification.

Verification is different. Verification is -- well, let me just give you an example. A person shows up to work. They slide their identity card into the time clock and they put their finger on the sensor. That's verification. So there the time clock is saying, Does this fingerprint match the individual who is defined by what's on the card? So that's different from the identification process.

Q. Do you know if the time clocks used by Speedway used verification or identification?

A. I don't recall that point.

Q. Do you know what the false acceptance rate is for the TimeLink and Kronos time clocks?

A. Off the top of my head, no.

Q. Is it -- do you agree that it's possible that time clocks used by Speedway potentially could confirm a user or authenticate -- sorry. Bad question.

Do you know if the time clocks used by Speedway could potentially identify or verify a user incorrectly? Like if Mr. Ficzko and I had a similar finger -- set of finger ridges and I put my finger on it, is it possible that the clock could think I was Mr. Ficzko clocking in?

A. That is possible.

Q. How did these -- now I'm asking about the Speedway time clocks. How do those time clocks match a user to a fingerscan?

A. There is a comparison between the template which has just been taken, so the live template. That is compared in the identification case with all of the registered fingerprints, and in the authentication case it's compared with just the employee here who has swiped their ID card.

Q. And do you know ultimately, so after finger template to finger template is matched, how is that then linked back to an individual, if at all?

A. In the authentication case, the individual has been signalled by the card, and these devices are networked, and so the clock may have a database of employees or the clock may ask essential server for information as to which person this is, so either of those is possible.

Q. Okay. [redacted]

A. Yes. I have that up.

Q. Okay. It says:

[redacted]

A. I see that.

Q. I have a very basic question first. There is no citation here. How do you know that

Speedway used those time clocks?

A. That was provided to me by retaining counsel.

Q. Do you know what kinds of sensors these clocks use, by which I mean acoustic, capacitive, optical, some other kind?

A. So there are three; the TimeLink, the Kronos -- the two Kronos are using the Sagem reader, and I guess the Syntel is using a different one, and these are optical devices.

Q. Other than this case, do you have any experience with optical sensors in time clocks?

A. I have lots of experience with optical sensors in my biomedical engineering work. This is the first case I've been involved with about time clocks.

Q. In the last ten years how much of your time have you spent working with optical sensors? Just by percentage.

A. This year probably 40 percent. Earlier than that, less.

Q. How much less? Less than ten percent?

A. Maybe ten percent is a reasonable number for previous years, but I don't have that area -- I mentioned that I'm doing work with the University of Arizona and I hope there will be a publication about that, but as of today there is not.

Q. [redacted]

So is it your opinion that a fingerprint was captured by the fingerprint reader used in the TimeLink 3100 and the Kronos 9000 and 9100?

A. Yes.

Q. And that opinion was based on the methodology you described in paragraph 13 where you said what you did?

A. Yes.

Q. Okay. Go to paragraph 17, please.

A. I have that up.

Q. Here you write:

[redacted]

Q. People who will do things like approve time cards for payroll, right?

A. Yes.

Q. Is this document the entire basis for your opinion in the opening report that the TimeLink clocks collect a fingerprint?

A. No.

Q. So what else do you base that opinion on? Remember, this is just about your opening report.

A. Yeah. So my opinion that this is recording a fingerprint and it's using the fingerprint reader comes from not only that particular document but also my understanding having worked in the field of what the word fingerprint means.

To me it's plainly obvious that this is a time clock with a fingerprint reader on it. And why is it so obvious? Well, because I have worked on fingerprint readers and I am familiar with the literature, and the device that's pictured in that document is a fingerprint reader, and I am baffled by how there is controversy about that.

Q. So your opinion is based on the user manual and your experience in the field, correct?

A. Yes.

Q. That's all?

A. Well, as I say, I've been doing biomedical engineering for 30 years. I've worked on a large fingerprint project during which everyone in the team referred to it as a fingerprint reader, and that fingerprint reader appears to have the same function as the clock we're talking about here.

Q. Okay. Go to paragraph 19 of your opening report, please.

A. Okay. I see that.

Q. Does paragraph 19 state the entire basis for your opinion in the opening report that the Kronos 9000 and 9100 time clocks capture a fingerprint?

A. I think this is the same as what we just discussed. There is certainly user manual evidence that talks about fingerscan images, and my experience in the field backs up the -- what's in the user manual which is that this is plainly a fingerprint reader.

Q. Okay. I'm going to show you and mark as [redacted] which is the entire document. It's the full version of the document you cite in paragraph 19 for pages 51 and 93.

(Exhibit 8 was marked for identification.)

BY THE WITNESS:

A. Okay. I have that up.

BY MR. WOLFE:

Q. Can you go to page 51 of this document, please?

A. Okay. I am at page 51.

Q. [redacted]

A. What I've got is page 51. [redacted]

Q. I'm sorry. I mean [redacted]

A. Okay. Right. Let me go there.

Q. That was my fault.

A. I'm sorry. What was your question? I have got the Bates number now.

Q. [redacted]

been instructed about how the BIPA uses these words is fingerscan, that's the process that you get a fingerprint from.

Q. Can we go to [redacted] in that document.

A. Okay. I've got that page.

Q. [redacted]

A. Yes. So you see in the beginning of that [redacted]. So that's the process, and so as a result of that process you've got fingerprints, and that's what is converted into a template and the template is then matched against stored information.

Q. The template is matched against the stored template?

A. That's right.

Q. [redacted] if I didn't say that already.

Do you understand that Speedway also

Q. Do you have any reason to disagree with that?

A. No.

Q. So is it your opinion that the devices Speedway used stored an image like the one in Figure 1 of the ink fingerprint?

A. I'm sorry. Could you repeat that question?

Q. Is it your opinion that the devices/time clocks used by Speedway store an image like the ink fingerprint shown in Figure 1 to Mr. Minta's opening report?

A. Yes. They have to because they need to compute the template.

Q. How long is that image stored?

A. I don't know.

Q. Is it stored permanently in solid state memory?

A. I don't have that information.

Q. You don't know one way or the other?

A. I don't know.

Q. Based on your experience in biometrics, that would be unusual, right?

A. It would be, but, you know, I don't

A. Yes.

Q. We established already that the TimeLink and Kronos devices both use the Morpho scanner, right?

A. That's my understanding.

Q. What is that understanding based on?

A. Retaining counsel told me.

Q. The Morpho scanner requires the user to put their finger in a fixed precise place, correct?

A. I would need to look at the document about that. I don't have that information off the top of my head.

Q. Okay. Let's go back to I think it's Exhibit 6 which is SSPA00001. And go to -- I may have my exhibit numbers wrong, but I'm talking about the TimeLink User Manual.

A. Yes, I have that.

Q. Go to page SSPA0004 again, the same one you relied on in your report, okay?

A. I have that.

Q. Do you see the Tip there in the center left of the page?

A. I do.

[redacted]

A. [redacted]

Q. Okay. Is it possible to enroll on a fingerscan device by using a body part other than the tip of your fingerpad?

A. Most of the body does not have the ridges and valleys that you find on the hands, and so I think that most of the body one could not use for that purpose. The ridges are evolved for the use of the hand.

Q. Are there parts of the body that you could use to enroll in a device? Because you said most of the body.

A. I don't know whether there is -- whether our toes have the same kind of ridges and that would be the only place that I would not know. But my arm, for example, that would not work because it just doesn't have the ridges and valleys.

Q. What about a knuckle?

A. That seems -- that would be very different data than what the device is looking for, so I wouldn't be optimistic that that would work.

Q. Have you ever heard of such a thing?

A. No. When people are trying to defeat these types of devices, it's more the, you know, spoof finger, you know, made with a mold.

Q. My question was, have you ever heard of someone who could enroll on a time clock by using their knuckle or a different part of their hand or the back of their finger?

A. I have not heard of that.

Q. Have you ever used a fingerscan time clock in the course of your employment?

A. I have not.

Q. So staying on the topic of the Morpho-enabled devices, whatever image is captured can be no larger than the scan surface.

Do you agree with that?

A. I wouldn't put it that way.

Q. How would you put it?

A. The size of the image is going to be determined both by the dimensions of the scan surface and also by the resolution of the reader, so it's not just the scan surface.

Q. Let me simplify it. Can you look at Exhibit 10 again?

A. Can you tell me which one that is?

Q. [redacted]

A. Okay. I have that one.

Q. Okay. [redacted]

A. Yes. I see that.

Q. And this isn't based on the document, but based on your experience, under the scan surface is an optical sensor so there has to be some kind of equipment underneath the scan surface to capture the image, right?

A. There does.

Q. And what kind of equipment would that be generally?

medical imaging.

Q. We've been talking about the Kronos and TimeLink technology. Just to make sure that we're on the same page, you agree that those both use Morpho hardware inside and functionally for our purposes they're the same, right?

A. That's my understanding.

Q. Okay. I want to ask you just a few questions about the Synel clock.

Does the Synel clock require the user to put their finger on a fixed precise place?

A. I don't know. I'd need to look back at the manual. I don't have that information in my head.

Q. Do you remember, does it capture a roll or a swipe?

A. I don't believe it's a roll and I don't believe it's a swipe. I think it's the same user experience as the other three time clocks. That's just off the top of my head.

Q. Do you know how large the scan surface of the Synel device was?

A. I do not. Oh, I'm sorry. I take that back. So on my page -- on my paragraph 22 we

Q. This paragraph appears to address the distribution of fingerprint data from time clocks to other network locations.

Do you agree with that?

A. Yes.

Q. Does paragraph 18 state the entire basis for your opinion in your opening report regarding the TimeLink devices distributing fingerprint data?

A. The documents I reviewed and quote here certainly indicate how -- it indicates that these devices are capable of distributing the information. I also understand from doing engineering for 30 years that there would be a need for that to take place in order for the system to work properly, and I also saw in Kostas Mallias's declaration that he testified about this.

Q. Let's go one sentence at a time. So it says:

[redacted]

That's not an important distinction in your mind, the difference between a partial and a whole?

A. It's clear that the fingerprint information that is obtained by a sensor can only be from the part of the finger that the sensor is in contact with, and so I see that as a distinction for like a rolled fingerprint with ink, but my point is that I had never heard of Mr. Minta's definition of fingerprint in all the time I've worked on this, and so I went back to the standard textbooks and I found that they all used the word fingerprint in the same way that I was instructed that BIPA used it, and so that's why I disagree with Mr. Minta's definition.

Q. Okay. And Mr. Minta goes on to write:

[redacted]

Is that consistent with what we talked about before in that the image typically would not be kept in the persistent memory, instead the features would be extracted and would be converted to a template?

A. What has to happen for the device to work minimally is that the image fingerprint has to be acquired and that has to go to a memory so that the microprocessor can create the template.

After that the device may or may not throw away the fingerprint image data, but the data has to exist for long enough for the microprocessor to do that feature extraction into the template.

Q. And that would be for a fraction of a second, correct?

A. If that's how fast the microprocessor is and how complicated the template algorithm is.

Q. Okay. Typically in a consumer user experience, you would want it to be less than a second, correct?

A. In the device I worked on, you do not want to be annoying the user by having a long period for authentication.

Q. Can you think of any reason why fingerscan time clocks would be different?

A. So time clocks are also used by humans who will get frustrated if they have to wait a long time for the template's algorithm to be executed.

Q. Okay. On the next page there is an illustration, Figure 2. Do you take any issue with that figure?

A. In what sense? I'm sorry.

Q. Do you think it's accurate?

A. If the sensor has -- if the sensor is of the size depicted, then it could be accurate. I mean, it's just a question of how big is the sensor, and so I'm not sure which device Mr. Minta is talking about here.

Q. Okay. [redacted]

MR. FICZKE: Where are you looking at?

MR. WOLFE: I'm paraphrasing from the last paragraph on 14 and the first paragraph on 15. So I'll rephrase it.

BY MR. WOLFE:

Q. [redacted]

[redacted]

A. There are various ways of doing the feature extraction to make the template from the fingerprint, and those features that constitute the template are what the machine looks for, and I guess Mr. Minta is using the word pattern to describe the template. So the matching is done on the template which will list the features formed from the fingerprint.

Q. Is that the same thing as an impression of the ridges of the fingertip unique to each human being and used as a means of identification, which is the Chambers Dictionary definition?

A. That's the definition of fingerprint.

[redacted]

The template is not the fingerprint. It's a calculation based on the fingerprint.

Q. The template is a list of the features found in the fingerprint, right?

A. I think that's fair.

Q. Do you know what that list looks like?

A. Well, that varies between manufacturers, and so, you know, minutiae points would be an example that is frequently used. Also things like the direction of all the ridges, that's a commonly used thing, where whorls end. There are a variety of ways to do the calculation of the template.

Q. [redacted]

A. Okay. I have that one up, 31.

Q. Okay. Here you write:

[redacted]

A. Yeah. I guess the company is now IDEMIA, but it was Sagem, yeah.

Q. And then you say, [redacted]

I'm wondering why you said [redacted] What would possibly be wrong with that? I mean, MR. FICZKE: Objection. One second, Dr. Daft. Objection; compound question.

BY MR. WOLFE:

Q. I'll ask it again.

MR. FICZKE: Yeah, if you can fix it.

BY MR. WOLFE:

Q. You believe what's initially collected is a fingerprint, correct?

A. Yes.

Q. And is it your understanding of Mr. Minta's opinion that he does not think a fingerprint is initially collected?

A. That is my understanding, yes.

Q. And when we get to pages 25 to 27, he's got a detailed description of how the devices work. And my question is, other than his opinion that what's initially collected is not a fingerprint, do you disagree with anything else in his description of how the devices work?

A. I disagree with -- well, I think that his description here supports my conclusion that the devices are collecting and storing biometric information, but that biometric information is the template.

is inaccurate?

A. I don't see a problem with Figure 12. I don't know its prominence, but it squares with my understanding of how these devices work.

Q. Okay. Look at Figure 13. Based on your experience and education, do you have reason to believe that Figure 13 is inaccurate?

A. I'm trying to see what the difference between 12 and 13 is. Currently I'm thinking that it's just the red X on the template encryption or rather the matcher algorithm. I mean, from the -- for the purposes of what's at issue here, again you see a sensor collecting data which to me is obviously a fingerprint.

That has to get stored in memory so that the CPU can turn it into a template, and I see at the top right again template storage. So if this is an accurate representation of what goes on inside the device, then it's supporting my opinions.

MR. WOLFE: New exhibit.

(Exhibit 13 was marked for identification.)

MR. WOLFE: So 13 is document

Q. What is that reason?

A. An image -- in order for the device to work, the image must be stored because data must be provided to the microprocessor to calculate the template, so the image must be stored.

Q. And when you say stored, you're referring to the transient image that would exist for less than a second while feature extraction takes place, right?

A. What I'm saying is that regardless of how long it's stored for, it has to be stored or the device wouldn't work.

Q. But like we talked about earlier, it would be very typical for an image to be captured, the features extracted, and the image discarded, right?

A. Yes. I think that typically is a way these devices work.

Q. And that process takes less than a second?

A. I think that's fair, but I disagree with the statement no images are stored at all within the Kronos system because if that's true, the device can't work.

Q. It has to store the image briefly in order to extract the features is your opinion?

A. Yes. I mean, that's how it has to work. The microprocessor has to have data to work with because the template is a calculation from the fingerprint image.

Q. Okay.

A. [redacted]

Q. I understand. And that process would take less than a second?

A. Typically it could.

Q. Now, the IAFIS system actually does store fingerprint images, right?

A. That's how it started, yes. And so that is a -- I agree with Kronos that there are differences between IAFIS and the Touch ID, [redacted]

Q. Look at the diagram at the bottom of the page.

MR. FICZKE: Is that the Step 1 diagram?

MR. WOLFE: Yes, sir.

BY MR. WOLFE:

Q. Is that diagram accurate from, you know, a basic perspective of how the technology works?

A. It is beyond me how the technology could work if the fingerprint was not stored so that the template could be produced from it.

Q. Okay. And then let's go, let's break it down a little bit. [redacted]

Do you think that part is accurate?

A. Yes.

Q. [redacted] So your opinion is that the fraction of a second capture is equivalent to storage; is that right?

A. The word storage doesn't have inside it the fingerprint to the template. [redacted]

BY MR. WOLFE:

Q. And the template is a list of features formed from the fingerscan based on whatever algorithm is in play in these devices?

A. Yes. The template is a computation of let's call it the essence of what the fingerprint has.

Q. And I don't want to ask you right now about your opinions about recreating the fingerprint. We'll get to that.

[redacted]

Is there anything inaccurate about that?

A. I don't know how the device works. [redacted]

[redacted]

That's my speculation as to what that -- the first part of the Step 2 sentence means.

Q. Okay. Do you disagree that a template is a mathematical representation?

A. No. I think that's a fine description of template.

Q. Are you aware if templates -- templates are stored in the system somehow, right?

A. Yes, because otherwise they couldn't work and, you know, Mr. Minta's report has diagrams including template storage.

Q. Do you know, are they stored in a table, something like a CSV file?

A. So I don't know. But from my experience with embedded systems -- this is an embedded computer system -- I would doubt that the template storage is a CSV file, but honestly I don't know.

Q. You don't know what kind of file it would be stored in?

A. I would expect that on an embedded system it would not be stored in a rather

Do you see that?

A. I do.

Q. My question is, after the long discussions we've had today and the documents that we've looked at throughout the day, is it still your opinion that there is no evidence to support a difference?

A. My opinion remains that finger scanning, as I state in my report, is the verb and fingerprint is the noun that you get from doing the verb.

Q. Okay. You didn't quite answer my question though. The question is, is there no evidence to support a difference or are you resolving the evidence to your opinion?

A. I see -- so let me answer it this way.

When -- every time that Mr. Minta is using fingerscan as a noun, I'm baffled because it's obviously a fingerprint.

Q. Is the fact that the sensors may scan something less than a full fingerprint not evidence that there could be a difference between a fingerscan and a fingerprint?

A. So let me answer that in two parts.

BIPA says that finger scanning is the verb to get the fingerprint, and a small sensor will produce a truncated fingerprint. It's still a fingerprint. It might not cover the entire finger, but it's still a fingerprint.

Q. Okay. Five minutes ago you told me there was obviously a difference between a partial fingerprint and a full fingerprint.

A. That's correct. It's fuller data, yes.

Q. Go to paragraph 42 and 43 in your report.

A. Okay. I see that.

Q. Your opinion here is that Ms. Jones's deposition does not support the statement in the Minta opening report; is that right?

A. I did not find that -- the information that's in Mr. Minta's report, I didn't find that in the deposition transcript.

Q. Okay. Do you have any other basis for the opinion in this part of the report?

A. The only opinion I'm giving here is that there isn't support for the claim on page 31 lines 23 to 24. There was a citation there and I followed up on the citation and I couldn't find what was being referred to, and there isn't a citation to a line of the deposition transcript.

Q. Thank you for your clear answer. Paragraphs 44 and 45 with the subheading, [redacted]

A. I see that, yes.

Q. Your opinion here is that the statement in Mr. Minta's opening report is inconsistent with Kostas Mallias's declaration; is that right?

A. It is inconsistent, that's correct.

Q. And the basis for that opinion is your review of Minta's opening report and Mallias's declaration?

A. That's -- so I guess that there is a couple of parts to this. Other citations show that the database sharing is possible. This was one piece of evidence that it had actually happened, and my engineering background suggests that the networking capabilities of these time clocks would be used for backups.

So I suspect that's not the only time that the templates moved from a clock to the central server or back in the other direction, but these citations I have here are one example that I saw in the evidence.

Q. Thank you for that. And we talked about that earlier, right? [redacted]

A. That's right.

Q. Okay. Is there any other basis for this opinion other than what's in your opening report and what we talked about earlier and the statement in your rebuttal?

A. The other thing I would say is in order to run a corporation with a lot of convenience stores, backup is necessary. And so I would be very surprised if these time clocks were not -- you know, if the company did not use the networking capabilities built into the time clocks for backup purposes.

Q. What experience in biometrics do you have that Mr. Minta does not?

A. I don't know that I can answer for

Q. Your opinion is that it is not impossible to reverse engineer a fingerprint from a template; is that right?

A. My opinion is that it is not impossible to reverse a template into a fingerprint.

Q. Do you have some ideas about how it could be done?

A. Yes, and those are cited in my report.

Q. One of them involved invertible neural networks, right?

A. That's correct.

Q. Are you an expert in invertible neural networks?

A. I have been working in neural networks, I hate to say, since 1990, so this is a variety of neural network that I'm familiar with.

Q. What does it mean to be an invertible neural network?

A. It means that there is a forward process. In this case the forward process is the mathematical calculation from the fingerprint to the template, and what the neural network is doing is learning, as in machine learning, how to do the reverse process, going from the template to the fingerprint image.

Q. Can you describe your experience with invertible neural networks?

A. So invertible neural networks are actually the subject of one of the publications in my CV. I can find which one it is if that's helpful.

Q. Yes. I would like to know.

A. It is citation 19 on page 5 of my CV.

Q. Can you describe generally what that paper was about?

A. Yes. So the goal there was we have a situation, it was a medical imaging situation, and the -- we know what I'll call the forward problem.

So this is ultrasound tomography. Imagine it in breast imaging. You've got the breast in a water tank and there is ultrasound transducers surrounding the breast. We know how to solve that problem in the forward direction.

What I mean by that is given the tissue, we can predict what the data acquired by the sensors did, and we can do that reliably.

What is of great interest for medicine

is being able to do the inverse problem, which is going from the sensor data back to the tissue characteristics of the breast and being able to make an image of the breast.

So what we were doing in that work is parallel to the situation with the fingerprint image and the template. So in this situation I'm going from the acquired data back to an image of the breast, given that I know how to do the forward problem. So the neural network learns the inverse problem, which I can't do.

So in the same way, with the fingerprint obviously we know what the forward problem is because that's just the software being executed by the microprocessor, and the inversion in the invertible neural network is teaching by machine learning that network to go in the opposite direction. That's how this work is similar to inverting the template back into the fingerprint.

Q. Are you aware of anyone who has reverse engineered a fingerprint image from a template using invertible neural networks?

A. I'm not aware of that. I have another citation not using invertible neural networks where the fingerprint image is being produced from the template.

Q. When you refer to that citation, are you referring to the article Fingerprint Image Reconstruction from Standard Templates by Cappelli and others?

A. Yes. So that's peer reviewed actually in a very prestigious journal, the IEEE Transactions on Patent Analysis and Machine Intelligence.

Q. Okay. We'll get to that. You also mentioned the use of artificial intelligence in your rebuttal?

A. Yes. And to be clear, artificial intelligence these days is sometimes used synonymously with neural -- actually often used synonymously with neural networks.

Q. Is that also true of the term deep learning?

A. Yes. All of those terms are kind of mushed together. Now, it's -- basically what all of that means is I know how to do the forward problem. I know how to go from the fingerprint to the template.

I am going to show the system -- which we can call a deep learning device, a neural network, or an artificial intelligence. I'm going to show it what are examples of fingerprints and templates, and from that training experience, this AI is going to learn how to invert.

Q. Got it. So you mentioned invertible neural networks, artificial intelligence, and deep learning, which I understand you to be saying are all approximately the same as being what you just described; that's how you would do it in a general --

A. That's right. They are all learning systems and those terms are -- I mean, 20 years ago those terms meant different things, but these days I think it's lost some precision. But all I'm meaning is it's a learning system that you train.

Q. Got it. Now, you mentioned in passing just now the paper by Cappelli and others. We'll talk about that in a minute.

Do you have any other ideas about how a

fingerprint could be reverse engineered from a template?

A. No. I think between machine learning algorithms and what Cappelli shows, that's what's backing up my claim that it is not impossible to do.

And I should add one other thing, that the capabilities of these AI systems are advancing with extraordinary speed. So it is very possible that if it's too hard today, that it won't be too hard in six months.

Q. Sure. Okay. So have you ever seen the Cappelli article before you found it in connection with this project?

A. No.

Q. Have you read any other papers, studies or publications on the topic of fingerprint image reconstruction from templates?

A. In one of the standard textbooks that I cite, I think it's Jain's book, there is a whole section that is entitled Attacks on the Template Database. So, in other words, this is some actor that wants to break into the biometric system, and so in that section in that monograph there is some other information on converting templates to fingerprint images.

Q. And in that chapter in the Jain textbook, J-a-i-n, other topics besides reconstruction of templates are addressed, right?

A. That's correct.

Q. And it mentions a whole bunch of methods of attacking the database and utilizing the information in the database, right?

A. Yes.

Q. How long is the portion of the Jain chapter on template reconstruction?

A. I see that the -- I'm just reading from my report. I see that attacks on the template database is 18 pages long.

Q. Okay. And then the portion of that template reconstruction is something less than 18 pages?

A. Yes, I think so.

Q. Okay. So tell me about the Cappelli article and how they purportedly reconstructed fingerprint images from templates.

A. Well, they did examples of

reconstructing fingerprint images from template data.

Q. Do you have any firsthand experience with that?

A. I have not attempted to reconstruct fingerprint images from template data. However, because I have been a neural net person for a long time, I know exactly how to do it.

Q. Okay. How would you do it?

A. I would get a large database and I would set up a neural network or actually a variety of neural networks and I would train them on that data, and then I would validate the result by showing it template information that it had not seen in the training setting.

Q. And if you wanted to train a neural network to reconstruct fingerprint images, you would need to know about the algorithm that is operating on the finger to create the original template, right?

A. Actually no. All I would need is examples of fingerprints and their corresponding templates. I would not need to know what the algorithm was.

Q. You could back out the algorithm?

A. It's possible. I wouldn't put it quite like that. The neural network eventually after training understands what the algorithm is. But I would not -- in order to break into this system, I would not need, for example, the source code running on a Kronos microprocessor. I would only need the fingerprint data and the template data.

Q. Okay. And within this database all the templates would have to be constructed the same way, right?

A. Yes. So the machine learning system is learning one specific algorithm. It would have to be repeated if there were a different algorithm in play.

Q. So the templates you would have would be -- I'm not going to use the right terms. They would be in some sort -- I mean this in a colloquial sense.

The templates that you would have would be in some code, right? Like the first part of the template corresponds to X, the next part of the template corresponds to Y, and eventually if you have enough of them, you can -- and the original fingerprint images, you can figure out how to reconstruct by teaching the machine that this template came from this image and this is what the code is?

A. That's right. I mean, that's true and it's actually true even independent of how the template information is encoded. So you were asking earlier about how that data is stored. This approach doesn't care about how that data is stored.

Q. What do you mean by that, doesn't care about how the data is stored?

A. What I mean is that if the template is stored in a CSV file as you had asked me about before, then this approach works. If the template is stored as raw binary data, this approach would also work.

Q. Are there other ways the template might be stored?

A. Yes. There are -- I mean, the encoding of that template data could be done in many, many different ways.

Q. Could it be stored in a text file?

Q. Binary format is like zeroes and ones, correct?

A. That's right, and obviously also there are many ways to do the encoding. By saying it's binary format, really what's meant there is it's not human readable.

Q. Okay. Would a human ever have occasion to read a fingerprint template?

A. If they were attempting to attack a biometric system, yes.

Q. If you were a human, not a machine, who wanted to read a fingerprint template, what would you do?

A. There is software that allows the binary data to be represented in a human readable format. That's not what we were just looking at in Mr. Minta's expert report. What he's showing is binary data that's just read into a text editor.

So in the world of, you know, undermining biometric systems, you would be using a binary data editor.

Q. Okay. So a binary data editor is the software that you just described?

A. Yes. And there are plenty of examples of that type of software.

Q. Okay. And the binary data editor converts the binary template data into a human readable format?

A. Yes. It reads the binary information and it turns it into typically hexadecimal data, and hexadecimal data is human readable.

Q. What does hexadecimal data look like?

A. It looks like the number zero up to nine and it also includes the letters A through F, so it's running on normal numbers of base ten. Hexadecimal means base 16.

So it's not just the normal numbers. We have to use six letters as well, and those are traditionally the first six letters of the alphabet.

Q. Okay. So if I had a fingerprint template and I put it through a binary data editor and converted it into hexadecimal, I would then have a string of letters and numbers A through F, zero to nine; is that right?

A. Yes, it is.

Q. And then what would I do next to read have four bytes for each hexadecimal letter. So you divide those figures by four and that would be the size of what you would see on the screen.

Q. So if I had a 400-byte template and I converted it to hexadecimal, I would have a 100 character template in recognizable human characters, letters and numbers?

A. That's correct.

Q. Like a really long driver's license?

A. Yes.

Q. So Cappelli was able to reverse engineer the templates knowing the algorithm in the laboratory on an open system; is that right?

A. Yes. Cappelli is doing research where he knows what the format of the template is, so the aspect of the template format has been removed from the discussion. So he's answering the question of can we reconstruct from a template for which we have the format? And that's different from the neural net approach where the format is irrelevant.

Q. Got it. So Cappelli sort of has an advantage over the neural network approach, right? He already knows what the format is?

doesn't apply here.

Q. Okay. Templates are the result of feature extraction, correct?

A. I think that's fair.

Q. And a template contains some lesser amount of data than the original image, correct?

A. Yes. We can see in Table 1 of the paper which I guess is on page 1492, this is showing the type of information that's in the template.

Q. So as part of the reconstruction process, the image that is reconstructed is going to be missing some information that would have been in the original image; is that right?

A. Well, that's where if you remember many hours ago we were talking about compressed sensing, how a digital camera can produce a resolution that's much higher than its sensor's resolution.

While the template is much smaller than the image, if it's got the key information and if the algorithm or the learning system is clever enough, then that is resulting in a synthetic fingerprint of good quality.

Q. Did Cappelli and his coauthors use that method?

A. Cappelli and the coauthors use the template data and they invent an algorithm that analyzes the template data and creates a synthetic fingerprint image, and then they evaluate how good that image is.

Q. And ultimately they conclude that it would be unlikely to fool a human reviewer but potentially could fool the same system; is that right?

A. That is what is stated in the abstract, and I have no reason to doubt that in 2007 that is what they concluded. So a high chance of deceiving state-of-the-art commercial fingerprint recognition systems, I think that's important for this case, because we're not talking about a human expert in fingerprints looking at the data. We're talking about can the machines be deceived.

Q. Is the reconstructed image transferable from one system to another? So if I reconstruct an image from the TimeLink system, can I go use it on the Qualcomm phone?

A. I think so because it's just the scanned image, and so that is far more doable than, you know -- if you don't know what the fingerprint template is, once you've got it back to an image, I think you can use it in other systems far more easily.

Q. But the reconstructed image is based on reversing the algorithm essentially, right?

A. I wouldn't put it that way. What they've done here is they have made an algorithm that understands the template and predicts the image, so it's through their understanding of the characteristics of fingerprints.

So the reason I brought up the compressed sensing in the digital camera is it's the same thing. The small amount of data plus the knowledge of the algorithm is able to get back with some level of fidelity to the fingerprint image.

Q. Would it make a difference if the feature extraction method was different from one sensor to the another, like if one was doing minutiae and one was doing, you know, ridge flow?

would have to do that work again for a different feature extraction algorithm.

If I'm a bad guy and I want to make money by breaking into the system, I would choose the neural network approach where neither the feature extraction specifics nor the encoding of the data matter for creating the fingerprint image, the synthetic fingerprint image.

Q. And why did either of them matter?

A. The Cappelli paper presumes a certain format and a certain kind of feature extraction. So they're not trying to break into that system to make money.

They're interested in what is the algorithmic likelihood, so they've just subtracted the whole question of how is the template formatted and what's in the template. They've subtracted that. They know all of that, so that's not part of their work.

But if I'm a criminal, I would opt for the approach where it doesn't matter about the format and it doesn't matter about the feature extraction.

Q. It would require a lot of resources, right?

A. I disagree. The speed -- I mean, the amount of learning power that is available with commodity hardware, like let's say a desktop PC, the amount of learning power in that has improved at an extraordinary rate in the last five to ten years.

Q. Do you think it could do an invertible neural network of this power on a PC that I can buy at Target?

A. I think, I mean my point in my report is we can't make a statement that -- I disagree with the statement that inverting the template algorithm is impossible. I think that's incorrect, and I think this paper shows that algorithmically it's possible and I feel that a neural network approach could be very suitable for someone with nefarious intent.

Q. Okay. We've talked about the neural network idea. We've talked about Cappelli and his paper.

Do you have any other ideas about how a fingerprint image could be reverse engineered from a template?

A. I think there is some other information in that section of the Jain book that I cite, but my opinion is simply disagreeing with the blanket statement that reversing the template algorithm is impossible. That's my opinion. I disagree that it's impossible.

Q. Okay. Can you go to Mr. Minta's opening report, Figure 8.

A. Yeah, I have that.

Q. Okay. And Figure 8 is where you can see the circuit board?

A. Okay. Yes, I have that.

Q. It's on page 21, right? There is three photos of the interior of the time clocks?

A. Yes.

Q. [redacted]

A. That's right.

Q. How would you do that?

A. So the context of this is how much

effort is determined by how valuable the information is, but the procedure would be to use some means to attach to the points in the circuit, for example, the pings.

[redacted] This is a standard free scale microprocessor, very common device.

Q. Are you referring to Figure 8 here?

A. Yes.

Q. Okay.

A. So underneath that device there is a whole bunch of pins, maybe 100, 150 of them. So it is entirely feasible to interpose a connector between that chip and the circuit board and watch all of the signals coming out of that and into that microprocessor.

Q. To do that, you have to physically connect probes in the logic analyzer, right?

A. That's right.

Q. What do you do with the oscilloscope?

A. The oscilloscope would be useful initially in learning what goes where in the circuit. This could take some amount of time, [redacted]

[redacted]

Q. You said using the oscilloscope to learn what goes where in the circuit could take some amount of time?

A. Yes.

Q. How much time do you think it would take?

A. I can't tell you without having tried to do this, this procedure.

Q. Do you personally have direct circuit probing experience with a prefabricated board like this?

A. I do.

Q. What is that experience?

A. When I worked at Cephasonics, we had lots of circuit boards where we have to probe with a logic analyzer in just the way that I've been describing.

Q. And what kinds of projects were you working on when you were doing that?

A. That was like an integrated circuit, some that we designed, and so the goal of the work was to understand whether the integrated

Once we have the circuit doing what we want or mostly doing what we want, then I go off and work on algorithms or something. So there were times when I was doing a lot of this and times when I was doing none of it.

Q. So over the two years that you were at Cephasonics, less than ten percent of your time?

A. We were pretty good. We could make circuits that work. And so the amount of probing that needed to be done was probably less than ten percent, but it's just a skill. I mean, once you know how to do it, it's not like if I spent my whole day doing it, I'm better. It's more of just once you know how to do this thing, it's an ordinary engineering skill.

Q. At Cephasonics were you trying to reverse engineer other people's technologies so you could copy it?

A. No, but trying to figure out a circuit board that's not working the way you want is just the same.

Q. At Cephasonics you would have the schematic diagram to know how it should work, right?

A. That's correct, and I know that I can go to the free scale website and I can download a document that tells me exactly what every pin under that MX-1 chip does. So I already know all of that information. I don't need to figure that out.

Q. Okay. A schematic diagram would be really helpful, right?

A. The schematic diagram can be obtained by reverse engineering the circuit board, so if this is something -- if this is a project where resources are available, the schematic can easily be reverse engineered.

Q. Okay. A minute ago you said, I know I can go to the free scale website and I can download a document that tells me exactly what every pin is under the MX-1 chip.

A. MX-1, it's a microprocessor. So yes, free scale documents, they're products, and so that includes telling me exactly what every pin does.

Q. Did you actually do that?

A. If I were on this project, that would be one of the first things I would do.

Q. But you didn't actually do it on this project, right?

A. I have not had a device in front of me.

Q. Okay. And you didn't go to the DragonBall website and get the schematic diagram?

A. No, because that would only be useful if I were seriously reverse engineering the circuit.

Q. Your point is simply that it is -- in your opinion it is possible to reverse engineer the circuit?

A. I think I put it slightly stronger than that. Reverse engineering the circuit is completely doable by an organization with enough resources.

Q. Like the National Security Agency?

A. I don't know what they -- I don't know what goes on inside there, but I know that in many cases people reverse engineer circuits like this simply because there is an economic motivation to do so.

Q. All right. So do you agree with me that the schematic diagram would be helpful?

A. Yes, and I'm saying that one can reverse engineer the schematic diagram from the physical object.

Q. Why would you need the schematic diagram for reverse engineering from the object? I don't understand.

A. Well, it's certainly helpful to have the schematic. What I'm saying is there is nothing magical that needs to take place to go from that board and its components to the schematic. It's a bunch of tedious work but it's not hard.

Q. How many hours total would you estimate you spent at Cephasonics on direct circuit probing?

A. I don't recall, but I will reinforce that this kind of probing, it's just a skill. You learn it at some point and you can do it afterwards. It's not a magical skill. It's a standard engineering technique.

Q. Was it less than 100 hours?

A. I think so.

Q. All right. So looking at the photo on the right in Figure 8, where on the circuit board would you connect to the signals?

A. I think the correct answer to that is as many places as possible. So that would include places like if you look at the bottom left, you'll see some solar panels. So that's one place that's very easy to connect.

You would also connect to -- I mean, you see three large integrated circuits. You would connect to all of the pins of each of those circuits, and you would connect to as many other places as you can find.

Q. A circuit board can have multiple layers, right?

A. That's correct.

Q. And some signals can be on inner layers of the board?

A. Yes. And so when people are doing reverse engineering, they slice these boards up. That's how you figure out -- I mean, the board is made from a bunch of layers that are glued literally together and it is sectioned so that it goes back to the parts that go into making the circuit board.

So at that point you know what the

layout is everywhere, including in the internal layers.

Q. I'm a little confused by your last sentence. You said, At that point you know what the layout is everywhere, including the internal layers. At what point do you mean?

A. I'm sorry. Let me say that differently.

The way a multilayer board is made is from a number of layers. They're physically separate pieces that are in the manufacture and they're glued together. When you're doing reverse engineering, you use a precise saw to divide the board up so that you get back all of those pieces which were the input to the board's manufacture. Once you've sliced the board into those pieces, then you can see the layout for the entire board.

Also in doing reverse engineering there are techniques like taking an x-ray of the circuit board provides lots of helpful information, so this field of reverse engineering is incredibly sophisticated.

There were lots of standard techniques

that have been -- that are known for doing reverse engineering.  But certainly the fact that this board is probably multilayer isn't an obstacle to reverse engineering it.

Q.   You say the layers are glued together, right?

A.   That's right.

Q.   Are they covered in some kind of protective coating before they're glued together?

A.   It's laminated in a certain way so that -- I mean, you have to make it so the one layer's copper, the conductors, doesn't interfere with another layer's copper.  But they're laminated together with glue.  I mean, this is very standard technology.

Q.   What kind of saw do you use to separate the layers?

A.   There are lots of sophisticated saws. You know, one that works is a saw like the type of saw that's used to cingulate, which means divide up, integrated circuits.

There are other -- I mean, another way of doing it, perhaps simpler, is simply to take the circuit board and put it rotating like a sander, right? So you can just abrade a layer of the circuit board and then you'll see what's underneath it. This is standard procedure.

Q. Do you know how many layers this board has?

A. I do not.

Q. But you said it's likely a multilayered board?

A. That would be my guess.

Q. When you have a multilayered board like this, can you be sure that the visible or accessible signals are the signals that you need to access?

A. For purposes of reverse engineering, you don't need to know everything. Those three chips that we can see are the three black squares. If you -- and if are reading every pin of each of those chips, that's providing an enormous amount of information suitable for reverse engineering what's going on.

So you don't have to go after every last -- every last piece of copper. Doing that could well be sufficient.

Q. How much time do you estimate it would take for someone with a reasonably high degree of microelectronic skill to do what you just talked about?

A. I can't give a reliable answer to that. I have -- I mean, this is called a teardown. That's the -- I mean, that would be how you'd get all of the points. You can see teardowns.

Every time there is a new iPhone, the reverse engineering companies do a teardown and they find out everything about that product including what's going on inside the chips, which is much harder than what I've been describing, which is learning what goes on on a circuit board.

So I can't estimate the amount of resources needed to do it. I do have a lot of confidence that given enough resources, this is doable.

Q. From your experience in biosensing, do you have an opinion or knowledge about whether human finger ridges are regular and predictable by some equation that can be applied to them?

A. What you just said is true to some

extent and not true generally, so I'm not offering an opinion on that.

Q. When a fingerscan image is converted to a template for feature extraction, some information is lost, right?

A. Certainly, because the file size is smaller. But again going back to the compressed sensing thing, you can't conclude from the file being smaller that you can't invert the process. You can't say that that's impossible, [redacted]

Q. So your position is that although some information is lost, it can be recreated?

A. That's right, and the reason it's possible to recreate it, that's what Cappelli shows, and also I would take us back to the digital camera with the compressed sensing.

That file that the camera produces is tiny compared with the resolution, yet it's got all of the high quality photographs that the user wants. So simply making the data smaller does not mean that it's impossible to get back to the original data, in this case the fingerprint image.